Cybersecurity Incident Report:
Network Traffic Analysis

Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log.

The network protocol analyzer logs indicate that UDP port 53 is unreachable when attempting to access the website www.yummyrecipesforme.com. Port 53 is normally used for DNS traffic. The log analysis shows that ICMP error messages were returned from the DNS server with the message “UDP port 53 unreachable.” This indicates a failure in the DNS resolution process. It is likely that the DNS server is either down, not listening on port 53, or blocked by a firewall.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.

The incident occurred at 1:34 p.m. and 30.25632 seconds, when several customers of client organizations reported that they could not access the website www.yummyrecipesforme.com. Instead, they encountered an error message stating “destination port unreachable” after attempting to load the page.

The IT security team responded by running tests with the network protocol analyzer tool, tcpdump, while attempting to access the site. The resulting logs showed that DNS queries using the UDP protocol were sent to the DNS server at IP 203.0.113.2, but the server returned ICMP error messages indicating that UDP port 53 was unreachable.

The root cause is likely that the DNS service was not running or port 53 was blocked by a firewall, preventing proper name resolution. Further steps may include checking the DNS service status, verifying firewall rules, and restarting the service if necessary.